



(12)

EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
28.11.2001 Bulletin 2001/48

(51) Int Cl.7: H04L 9/08

(43) Date of publication A2:
28.04.1999 Bulletin 1999/17

(21) Application number: 98119629.8

(22) Date of filing: 16.10.1998

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(72) Inventor: Al-Salqan, Yahya Y.
Mountain View, CA 94043 (US)

(74) Representative: Browne, Robin Forsythe, Dr.
Urquhart-Dykes & Lord
Tower House
Merrion Way
Leeds LS2 8PA West Yorkshire (GB)

(30) Priority: 20.10.1997 US 954170
20.10.1997 US 955015

(71) Applicant: SUN MICROSYSTEMS, INC.
Mountain View, CA 94043 (US)

(54) Method and apparatus for encoding and recovering keys

(57) A key such as a private key or key password of a private key is encrypted for storage, and may be decrypted if the private key becomes lost or unavailable. The key is encrypted by encoding, for example, by hashing, private information such as mother's maiden name and social security number, and the result is used as a key to encrypt the private key using DES or another symmetric encryption technique. The encrypted key is again encrypted, for example using asymmetric encryption, using the public key of a trusted party such as the certificate authority that generated the private key. The result may be stored as a key recovery file by the principal of the private key or another party. To decrypt the key recovery file, the private key corresponding to the public key used to encrypt the key recovery file is used to decrypt the key recovery file, for example by asymmetric decryption. The result is symmetrically decrypted using a key obtained by encoding, for example, by hashing, the private information in the same manner as was used to encrypt the key. The result of this decryption is the key.

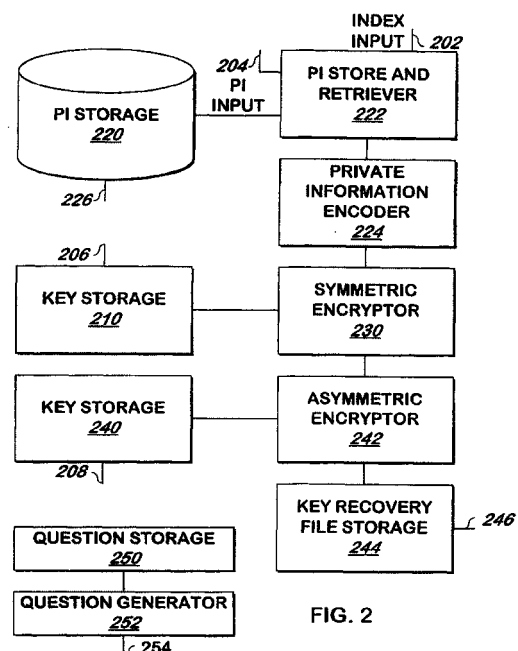


FIG. 2



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 11 9629

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
Y	US 5 557 765 A (LIPNER ET AL.) 17 September 1996 (1996-09-17) * column 17, line 30 - column 20, line 31 * * column 21, line 61 - column 29, line 52 *	1-44	H04L9/08
Y	MENEZES, OORSCHOT, VANSTONE: "Handbook of Applied Cryptography" HANDBOOK OF APPLIED CRYPTOGRAPHY, XX, XX, 1997, XP002177736 ISBN: 0-8493-8523-7 * page 389 * * page 394 - page 395 *	1-44	
			TECHNICAL FIELDS SEARCHED (Int.Cl.6)
			H04L
The present search report has been drawn up for all claims			
Place of search BERLIN		Date of completion of the search 27 September 2001	Examiner Carnerero Álvaro, F
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			

EPO FORM 1503 03.82 (P04001)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 98 11 9629

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

27-09-2001

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5557765 A	17-09-1996	US 5557346 A	17-09-1996
		AU 3321795 A	07-03-1996
		BR 9508548 A	03-11-1998
		CA 2197206 A1	22-02-1996
		CN 1158195 A	27-08-1997
		EP 0775401 A1	28-05-1997
		JP 10508438 T	18-08-1998
		US 6272632 B1	07-08-2001
		US 5991406 A	23-11-1999
		WO 9605673 A1	22-02-1996
		US 5745573 A	28-04-1998
		US 5640454 A	17-06-1997
		US 5956403 A	21-09-1999

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82